

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS

In The Matter of the Search of

[REDACTED]

Worcester, Massachusetts

M.J. No. 17-mj-4285-DHH

MOTION TO SEAL

The United States of America respectfully moves this Court to seal the search warrant application, supporting affidavit, search warrant, this motion, any ruling on this motion, and all related paperwork until further order of this Court. In support of this motion, the government states that the public disclosure of any of these materials at this juncture could jeopardize the government's ongoing investigation in this case.

The United States further moves, pursuant to General Order 06-05, that the United States Attorney, through undersigned counsel, be provided copies of all sealed documents which the United States has filed in this matter.

Respectfully submitted,

WILLIAM D. WEINREB  
Acting United States Attorney

ALLOWED David H. Hennessy U.S.M.J.

**Oct 31, 2017**

By: /s/ Karin M. Bell  
KARIN M. BELL  
Assistant U.S. Attorney

Date: October 31, 2017

## UNITED STATES DISTRICT COURT

for the  
District of MassachusettsIn the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)[REDACTED]  
Worcester, Massachusetts

Case No. 17-mj-4285-DHH

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

The premises at [REDACTED] Worcester, Massachusetts, more fully described in Attachment A.

located in the \_\_\_\_\_ District of \_\_\_\_\_ Massachusetts, there is now concealed (identify the person or describe the property to be seized):

Evidence, instrumentalities, fruits of crime and contraband of violations of 18 U.S.C. § 2422(b); 18 U.S.C. § 2251(a); 18 U.S.C. § 2252A(a)(2); and 18 U.S.C. § 2252A(a)(5)(B), as described more fully in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

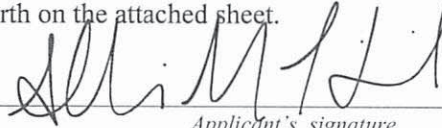
Code Section	Offense Description
18 USC §§ 2422(b);	knowingly persuade, induce, entice or coerce a minor to engage in sexual activity;
2251(a);	production of child pornography;
2252A(a)(2); 2252A(a)(5)(B)	receipt of child pornography; and possession of child pornography

The application is based on these facts:

Please see attached affidavit by HSI Special Agent Allison Haimila.

☒ Continued on the attached sheet.

☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

  
Applicant's signature

HSI Special Agent Allison Haimila

Printed name and title

Sworn to before me and signed in my presence.

Date: 10/31/2017

City and state: Worcester, Massachusetts

  
Judge's signature  
  
Chief U.S. Magistrate Judge David H. Hennessy  
Printed name and title



## UNITED STATES DISTRICT COURT

for the  
District of Massachusetts

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Worcester, Massachusetts

Case No. 17-mj-4285-DHH

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the \_\_\_\_\_ District of \_\_\_\_\_ Massachusetts  
(identify the person or describe the property to be searched and give its location):

The premises at \_\_\_\_\_ Worcester, Massachusetts, more fully described in Attachment A.

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Evidence, instrumentalities, fruits of crime and contraband of violations of 18 U.S.C. § 2422(b) (using a facility of interstate commerce to knowingly persuade, induce, entice or coerce a minor to engage in any sexual activity); 18 U.S.C. § 2251(a) (production of child pornography); 18 U.S.C. § 2252A(a)(2) (receipt of child pornography); and 18 U.S.C. § 2252A(a)(5)(B) (possession of child pornography), as described more fully in Attachment B.

**YOU ARE COMMANDED** to execute this warrant on or before November 13, 2017 (not to exceed 14 days)  
☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable David H. Hennessy  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30) ☐ until, the facts justifying, the later specific date of \_\_\_\_\_

Date and time issued: Oct 31, 2017 9:52 a.m.

City and state: Worcester, Massachusetts

  
Judge's signature  
Chief U.S. Magistrate Judge David H. Hennessy  
Printed name and title



AO 93 (Rev. 11/13) Search and Seizure Warrant (Page 2)

**Return**

Case No.:

17-mj-4285-DHH

Date and time warrant executed:

Copy of warrant and inventory left with:

Inventory made in the presence of :

Inventory of the property taken and name of any person(s) seized:

**Certification**

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: \_\_\_\_\_

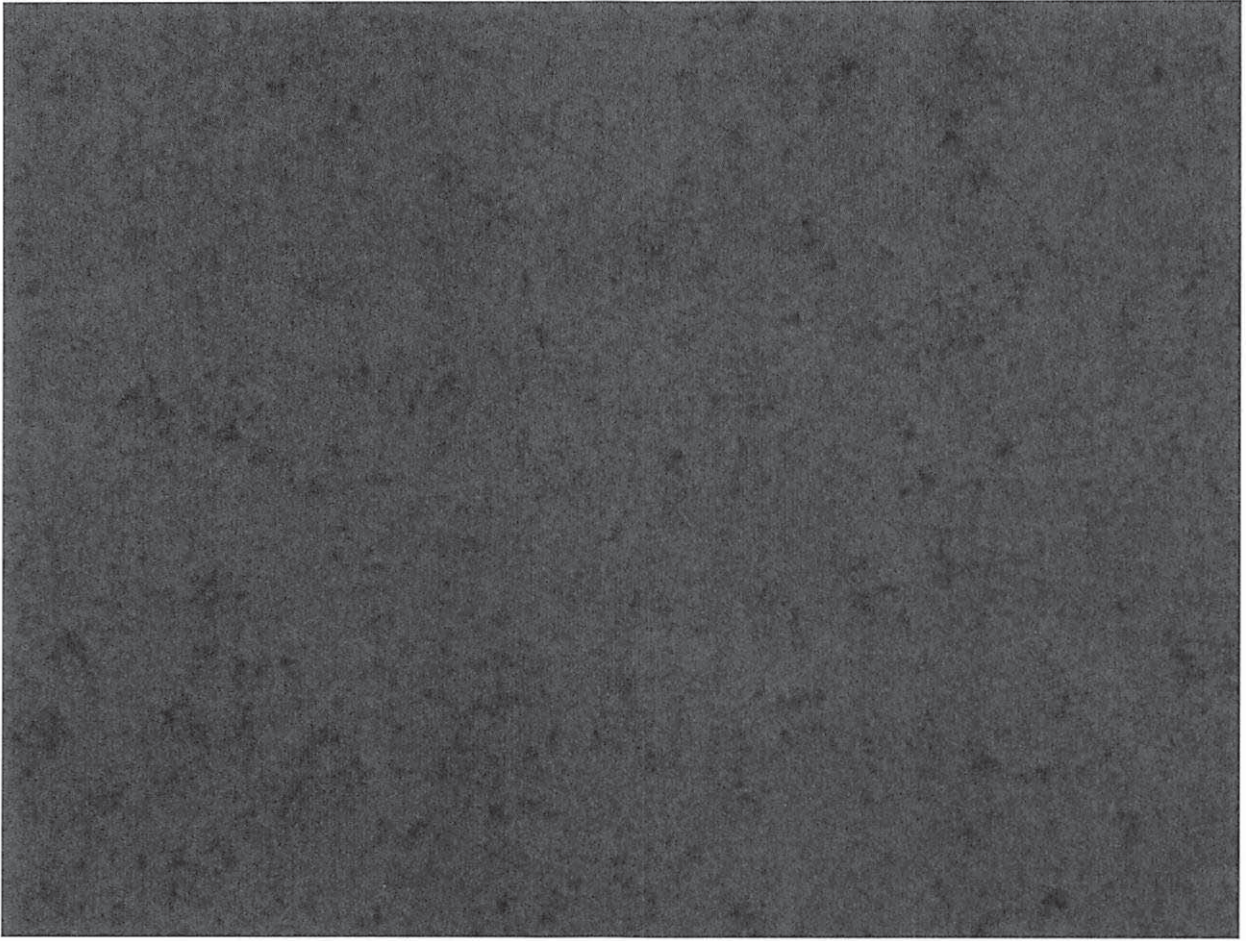
\_\_\_\_\_  
*Executing officer's signature*\_\_\_\_\_  
*Printed name and title*

## ATTACHMENT A

### The Subject Premises

The apartment located at [REDACTED], Worcester, Massachusetts is described as follows. The building itself is located at the intersection of [REDACTED] in Worcester, Massachusetts. It is a multi-unit apartment building. The first level of the building has a stone façade on all sides. The second and third floors of the building are covered with white vinyl siding. The roof is flat, except for a push out in front for the second floor which has a pitched roof. There are four (4) concrete steps leading to a front glass entry door accessible from the sidewalk on [REDACTED] Street. The glass entry door has numbers "[REDACTED]" marked in letters on the glass. There are also black "[REDACTED]" numbers affixed to the white door trim to the left of the door and another set of numbers above the door. Apartment [REDACTED] is to the right at the top of the staircase inside the main entrance (when viewed from the top of the stairs, which go in a circle separated by landings; when viewed from the street, apartment [REDACTED] is to the left). The door to apartment [REDACTED] has two gold deadbolts above a gold door handle. There is a "Welcome" sign with a black and white cat hanging from a wire from a screw in the door. There is a numbered parking lot and driveway for [REDACTED] which is located on the left side of the residence (the driveway is not pictured below).





## **ATTACHMENT B**

### **Items to be Seized**

1. Any and all child pornography, meaning any visual depiction, including, but not limited to, any photograph, film, video, picture, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct or such visual depiction appears to be of a minor engaging in sexually explicit conduct.
2. Any and all computers and all related computer equipment, peripherals, hardware, software, printers, data storage devices (e.g., thumb drives, zip drives, CDs, DVDs, floppy disks, digital cameras, digital memory cards, web cameras, camera phones, smartphones, xbox 360, other storage mediums such as Apple's IPOD line of products, and any other technology capable of storing digital images), as well as related instructions for operating the foregoing.
3. Records evidencing occupancy and/or ownership of the Subject Premises including, but not limited to, utility and telephone bills, envelopes addressed to the Subject Premises, and photographs of GUAVIN with and/or without other persons.
4. Records of correspondence or other communications (including, but not limited to, chatroom messages and e-mail) pertaining to or referring to: the coercion and/or enticement of minors: knowing possession and/or receipt of child pornography; and, production and/or attempted production of child pornography.
5. For any computer or storage medium whose seizure is otherwise authorized by this warrant (including smartphones), and any computer or storage medium that contains or in which is stored records or information that is otherwise called for by this warrant (hereinafter, "COMPUTER"):
  - a. evidence of who used, owned, or controlled the COMPUTER at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;
  - b. evidence of software that would allow others to control the COMPUTER, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
  - c. evidence of the lack of such malicious software;



- d. evidence of the attachment to the COMPUTER of other storage devices or similar containers for electronic evidence;
- e. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the COMPUTER;
- f. evidence of the times the COMPUTER was used;
- g. passwords, encryption keys, and other access devices that may be necessary to access the COMPUTER;
- h. documentation and manuals that may be necessary to access the COMPUTER or to conduct a forensic examination of the COMPUTER;
- i. records of or information about Internet Protocol addresses used by the COMPUTER;
- j. records of or information about the COMPUTER's Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;
- k. contextual information necessary to understand the evidence described in this attachment.



**AFFIDAVIT IN SUPPORT OF SEARCH WARRANT**

I, Allison Haimila, being duly sworn, depose and state as follows:

**BACKGROUND OF AFFIANT**

1. I am a Special Agent with the Department of Homeland Security, Homeland Security Investigations (“HSI”), assigned to the Resident Agent in Charge in the District of Connecticut. I have been so employed since 2009. I have received training in the area of child pornography (as defined in 18 U.S.C. § 2256) and child exploitation, and have, as part of my daily duties as an HSI agent, investigated violations relating to child exploitation and child pornography, including violations pertaining to the enticement of minors to engage in unlawful sexual activity in violation of 18 U.S.C. § 2422(b). I have also participated in the execution of search and arrest warrants, which involved child exploitation and/or child pornography offenses. As a federal agent, I am authorized to investigate violations of the laws of the United States and to execute warrants issued under the authority of the United States.

2. I am currently working with Connecticut State Police (“CSP”) and other law enforcement officers to investigate William Gauvin (“GAUVIN”), an adult male born in 1975, who, at the time of the offense conduct under investigation, was residing in Worcester, Massachusetts, for knowingly using and attempting to use a means or facility of interstate commerce to persuade, induce, entice, or coerce a minor to engage in unlawful sexual activity, in violation of 18 U.S.C. § 2422(b)<sup>1</sup>; production of child pornography, in violation of 18 U.S.C. § 2251(a)<sup>2</sup>; receipt of child

---

<sup>1</sup> Generally, 18 U.S.C. § 2422(b) criminalizes using a facility of interstate commerce to knowingly persuade, induce, entice or coerce a minor to engage in any sexual activity for which a person can be charged with a crime.

<sup>2</sup> Generally, 18 U.S.C. § 2251(a) criminalizes employing, using, persuading, inducing enticing or coercing any minor to engage in any sexually explicit conduct for the purpose of producing a visual depiction of such conduct or for the purpose of transmitting a live visual depiction of such conduct. . .

pornography, in violation of 18 U.S.C. § 2252A(a)(2)<sup>3</sup>, and possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B)<sup>4</sup> (the “TARGET OFFENSES”).

3. I subscribe this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the premises known as [REDACTED], Worcester, Massachusetts (hereinafter “SUBJECT PREMISES”), which is further described in Attachment A, for contraband and evidence, fruits and instrumentalities of the TARGET OFFENSES.

4. Based on the information set forth in this affidavit, there is probable cause to believe that the SUBJECT PREMISES contain items that constitute instrumentalities, fruits, and evidence of the TARGET OFFENSES as further specified in Attachment B.

5. The statements contained in this affidavit are based in part on information provided by other members of local, state, and federal law enforcement, my own investigation to include personal observations, documents and other investigative materials which I have reviewed, as well my training and experience as a Special Agent with HSI. Since this affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that evidence, fruits, and instrumentalities of the TARGET OFFENSES are located within the SUBJECT PREMISES.

---

<sup>3</sup> Generally, 18 U.S.C. § 2252A(a)(2) criminalizes the knowing receipt or distribution of child pornography in or affecting interstate commerce, including by computer.

<sup>4</sup> Generally, 18 U.S.C. § 2252A(a)(5)(B) criminalizes the possession of child pornography in or affecting interstate commerce, including by computer.

**PROBABLE CAUSE**

**Skype**

6. Skype is a free online service, currently owned by Microsoft Corporation, that is available for download as a program on computers as well as in app form for Internet capable cellular telephones. Skype uses cellular data or Wi-Fi to allow users to communicate with each other through voice calls, live video stream, and text messages that can include transmitting and receiving messages, photos, videos and other content. To use this application, a user downloads the application via the Skype webpage, or a service such as the Google Play Store onto a computer or other internet capable device such as a cellphone.

7. Once the application is downloaded and installed, the user is prompted to create an account by providing a first name, a last name, date of birth, and an email address. A Skype user must also create an account name or a username that can be any combination of numbers and letters as long as another Skype user is not already using it. The first and last names are submitted by the user and are not verified by Skype, and may or may not be the user's real name. The same user can create multiple Skype accounts.

8. Once the user has created a Skype account, the user is able to locate other users via a search feature, and the two parties can then communicate via voice, text messages and live video feed. They can also exchange files. I am also aware that the Skype program has a function built into it called "Video Snapshot." This function allows the user to take still photos of the person they are communicating with during a video call. These photos depict a still image of whatever the other person is doing on the video call when the snapshot is taken. These photos are then saved to a location on the user's hard drive.



### **PayPal**

9. PayPal is an American company that operates a worldwide online payment system, supports online money transfers, and serves as an electronic alternative to traditional payment methods such as checks and money orders. PayPal is one of the world's largest Internet payment companies and operates as a payment processor for online vendors, auction sites, and other commercial users, for which it charges a fee. Individuals can also use Paypal to transfer money from one person to another, which is called a "Friends and Family" transfer, and this service is free of charge. Individuals wishing to use the PayPal money transfer service must first register with PayPal with an email address and create a password. The user then has to supply an address and link a bank account and/or credit card with the PayPal account in order to transfer and receive money. Money sent to another individual through PayPal is withdrawn from the sender's bank account or credit card and sent to the intended recipient's PayPal account. The recipient can then transfer the money received through PayPal to the recipient's linked bank account for cash withdrawal. Transaction history is viewable from your PayPal account as well as the email contact information for the individuals with whom you have conducted transactions with in the past. Clicking on one transaction in the activity screen will allow a user to access his/her transaction history with that individual.

### **Instant Investigation**

10. On 03/15/2017, the CSP received notification from the Connecticut Department of Children and Families ("DCF") of a report of suspected child exploitation involving two minor siblings ages 17 and 15, Minor Victim 1 ("MV1") and Minor Victim 2 ("MV2"), respectively.

11. On 03/21/2017, CSP along with DCF interviewed the MVs mother, Dawn. Dawn stated that she was looking through MV1's iPhone. Dawn explained that she bought the iPhone for

MV1 and pays for the plan. Dawn stated that while accessing MV1's iPhone, she observed text messages from an unknown male to MV1. The text messages appeared within the Skype app on the iPhone. Dawn stated that the unknown male was identified via the contact information as "Will Wiggins." The text messages indicated that MV1 was possibly performing sexual acts for "Will Wiggins." Additionally, the text messages indicated that "Will Wiggins" was soliciting MV1 to engage in sexual acts with his younger sibling, MV2. Dawn explained that she also searched MV1's iPad and observed that MV1 was utilizing the Skype application to video the possible sexual acts for "Will Wiggins" while text messaging on the iPhone with "Will Wiggins." Dawn explained that MV1 also admitted to her that he performed sexual acts in exchange for payments via PayPal.

12. Dawn explained that she was able to take screen shots of some of the text messages between "Will Wiggins" and MV1, from MV1's iPhone, which she provided to CSP via e-mail. Dawn also created screen shots of a PayPal account she discovered on MV1's iPad which showed money that MV1 received from "william gauvin," which she provided to CSP via e-mail. MV1's PayPal account indicated that "william gauvin" had an e-mail account of [REDACTED]@gmail.com.

13. According to the screen shots, the text messages indicated that from approximately 10/27/16 to 3/22/17, "Will Wiggins" was regularly soliciting MV1 to engage in sexual acts with MV2, and to transmit images of the sexual acts via Skype in exchange for money sent through PayPal. The following are examples of Skype text messages between MV1 and Wiggins taken from the screen shots of the text messages that were provided to law enforcement by MV1's mother. According to Dawn, each of these screenshots came from MV1's iPhone.<sup>5</sup>

---

<sup>5</sup> Final forensics of MV1's iPhone are still pending.

14. On January 11, 2017, the following text messages occurred over Skype between MV1 and Wiggins:

Wiggins: touch his penis

Wiggins: Get naked

Wiggins: Take ur shirt off

Wiggins: brb one sec <sup>6</sup>

MV1: I'll take shirt off

Wiggins: Touch (MV2)'s penis

Wiggins: Haha play with (MV2)Wiggins: Come near him

Wiggins: Go play with (MV2)

Wiggins: Thanks let me send

MV1: Thanks for that, I'll see if (MV2) wants to do a chat again but it'd be the same prices or higher he isn't really down lately

Wiggins: Np ur fine<sup>7</sup>

Wiggins: Did u get

Wiggins: Sent 100 and 300

15. On January 11, 2017, MV1's PayPal account showed that he received \$300 and \$100 from william gauvin's PayPal account.

16. On January 26, 2017, the following text messages occurred over Skype between MV1 and Wiggins:

Wiggins: All is well we need to cam soon

---

<sup>6</sup> In my training and experience, "brb" stands for "be right back."

<sup>7</sup> "In my training and experience, "np" stands for "no problem."



Wiggins: (MV2) down or

MV1: we do and maybe something light soon

Wiggins: Cool

Wiggins: How much to hand out with u and him

MV1: probably 800 more if you want something remotely explicit for him its like at least a grand

Wiggins: Coil <sup>8</sup>

Wiggins: Was thinking around Feb break

Wiggins: So grand each

MV1: yeah ill ask him

Wiggins: Okay would he get nude

Wiggins: U taking a break from school

MV1: No I don't think so and I'm at school now

Wiggins: Oh okay

Wiggins: Would pay if he was cool with it

MV1: how much more I'm just not sure I could convince him to

Wiggins: Just ask and see what he is cool with

17. Between January 27, 2017 and March 2, 2017, "Will Wiggins" repeatedly asked for an "update on (MV2)". For instance, on February 6, 2017, the following text messages occurred over Skype between "Will Wiggins" and MV1:

MV1: yeah its annoying but im okay, no he (MV2) isn't down for it at the moment.

Wiggins: Okay

Wiggins: For nothing

---

<sup>8</sup> Agents believe he intended to write "Cool."

Wiggins: Not His Gig Not Even To cam

MV1: what do you mean?

Wiggins: Would he Skype with u again

Wiggins: Or is he retired

MV1: oh I don't know im hoping he will again but not right now at least I did talk to him

Wiggins: Cooo

Wiggins: When u wanna play on cam

MV1: whenever

Wiggins: Okay like five

Wiggins: (MV2) home or

MV1: he's downstairs but with a friend

Wiggins: Oh who is the friend

Wiggins: Snap some pics

Wiggins: Would \$\$\$

MV1: I don't really know ill see if their here

Wiggins: Haha recruit his friend

MV1: they actually just left to go on a hike im sorry

Wiggins: No worries

18. On February 23, 2017, at approximately 11:07 PM the following text messages occurred over Skype between "Will Wiggins" and MV1:

Wiggins: U on winter vacation

MV1: no only had till Tuesday

Wiggins: CT is different

Wiggins: U up now

(a call over Skype occurs for 24 seconds) <sup>9</sup>

Wiggins: (MV2) home

MV1: hey (MV2)s here I can show you him for a little but no touching him

MV1: ill call you in just a few

Wiggins: OK

MV1: how much\$?

Wiggins: What's ur costs

Wiggins: He sleeping or

Wiggins: 500

Call started<sup>10</sup>

MV1: hes sleeping 500 is good

Wiggins: Nice

Wiggins: Take it all off

Wiggins: Hot

Wiggins: What's on ur dick

MV1: wdym on my dick<sup>11</sup>

Wiggins: Nvm<sup>12</sup>

---

<sup>9</sup> The Skype call is indicated on the screen shots of the phone. It appears as an icon of a telephone with the words "Call, 24s" next to it.

<sup>10</sup> The Skype call is indicated on the screen shots of the phone. It appears as an icon of a telephone with the words "Call started" next to it.

<sup>11</sup> "In my training and experience, "wdym" stands for "what do you mean."

<sup>12</sup> "In my training and experience, "nvm" stands for "nevermind."



Wiggins: Lighting

Wiggins: Where is (MV2)

Wiggins: Hot

Wiggins: Where's is ur bro

Wiggins: Is ur bro near

Wiggins: Sexy

Wiggins: Nice

Wiggins: Show him

Wiggins: Hot

Wiggins: So close keep it on him

Wiggins: Hot

Wiggins: Show ur bro

Wiggins: Did he wake up

Wiggins: May I see him again

MV1: he did lol

Wiggins: Pretty please

Wiggins: Go in front of (MV2)

Wiggins: Haha cum on his bed

Wiggins: So close

Wiggins: Show his whole body

Wiggins: Haha pull his pants down

Call, 19min 2s<sup>13</sup>

Wiggins: No problem

Wiggins: all set

Wiggins: Get some rest

MV1: nice shot

MV1: paypal?

Wiggins: All set

Wiggins: Take care

19. Screenshots taken by Dawn, as well as PayPal records indicate that, on February 23, 2017, MV1's PayPal account received \$500 from william gauvin's PayPal account. Screenshots taken by Dawn, as well as PayPal records also indicate that between October 27, 2016 and February 24, 2017, MV1 received over \$3,000 from william gauvin's PayPal account.

20. On March 6, 2017, the following text messages occurred over Skype between "Will Wiggins" and MV1:.

MV1: sorry I fell asleep

MV1: want to chat tonight?

Wiggins: Sure (MV2) playing with you

MV1: not today but soon he wont show you bare cock though

Wiggins: np .

Wiggins: What will he show off

Wiggins: ?

---

<sup>13</sup> The Skype call ending is indicated on the screen shots. It appears as an icon of a telephone with the words "Call, 19min 2s" next to it. The text that occurred between footnotes 10 and 13 appears to have occurred during the Skype video call.

Identification of GAUVIN

21. In April 2017, CSP executed a search warrant on PayPal for the account of “william gauvin”. PayPal responded to the warrant with the following registration information:

User Info:  
First Name: william  
Last Name: gauvin  
DOB: [REDACTED] 1975  
Email: [REDACTED]@gmail.com  
Account Status: Open  
Account #: [REDACTED] 9760  
Account Type: Personal- Verified  
Time Created: Sat, 30 Jun 2007 2:33:55  
SSN: [REDACTED] -8437  
Email Addresses:  
[REDACTED]@gmail.com  
[REDACTED]@yahoo.com  
[REDACTED]@yahoo.com  
Phone Number:  
[REDACTED] -7377  
Billing Address:  
[REDACTED] Worcester, MA 01602

22. On January 10, 2017 at 10:50 pm Pacific Standard Time (“PST”), \$103.20<sup>14</sup> was sent from the william guavin PayPal account to MV1’s PayPal account.<sup>15</sup> One minute later, on January 10, 2017 at 10:51 pm PST, \$300<sup>16</sup> was sent from the William Gauvin PayPal account to MV1’s PayPal account. The PayPal records further show that, on February 23, 2017 at 9:10 pm PST (or 5:10 am on February 24, 2017 UTC), \$514.80 was sent from william gauvin’s PayPal

---

<sup>14</sup> It is my understanding that the additional \$3.20 is a 2.9% fee (plus an additional \$.30) charged by PayPal per transaction.

<sup>15</sup> 10:50 pm PST is equivalent to 6:50 AM January 11, 2017 Coordinated Universal Time (“UTC”). UTC is the same as Greenwich Mean Time, or GMT. UTC does not observe daylight savings time.

<sup>16</sup> The records do not appear to reflect a transaction fee associated with this payment.



account to MVI's PayPal account.<sup>17</sup> The IP address used to access william gauvin's PayPal account for each of these transactions was 68.187.230.172. In fact, the response from PayPal shows that between October 31, 2016 and March 2, 2017, the IP address predominantly used to access william gauvin's PayPal account was 68.187.230.172, and between March 3, 2017 and March 22, 2017, the IP address predominantly used to access william gauvin's PayPal account was 66.189.117.131.<sup>18</sup>

23. On or about April 19, 2017, the Massachusetts State Police ("MSP") provided an RMV photo of William GAUVIN that included the following information:

Massachusetts drivers license # [REDACTED] 1594  
 SS# [REDACTED] -8437  
 [REDACTED], WORCESTER, MA 01602

24. In April 2017, CSP served a court order on Google for subscriber information and IP history associated with the email address [REDACTED]@gmail.com, the email address linked to the PayPal account of william gauvin.

25. On or about April 20, 2017, Google responded to the court order with the following subscriber information regarding the email address [REDACTED]@gmail.com:

Name: bill Gauvin  
 E-Mail: [REDACTED]@gmail.com  
 Status: enabled

---

<sup>17</sup> Again, this includes a 2.9% transaction fee plus \$.30.

<sup>18</sup> Indeed, of the 113 logins to the william gauvin PayPal account from October 31, 2016 to March 22, 2017, only seven log-ins were from IP addresses other than the two IP addresses listed above. Six of those seven were IP addresses assigned to T-Mobile wireless customers indicating that the gauvin PayPal account was accessed via a mobile device, but not using a wireless network. The seventh IP address was assigned to Comcast and geo-location information indicates it was assigned to Fort Myers, Florida. In my training and experience the person accessing the gauvin PayPal account in this instance likely did so using wireless internet service while located in Florida. Also according to PayPal records, with the exception of one Web Login in November 2016, each time the gauvin PayPal account was accessed, it was accessed via a mobile device.

SMS: + [REDACTED] 7377

26. The Google response shows that the email address [REDACTED]@gmail.com is linked to the name “bill Gauvin.” The listed phone number [REDACTED] 7377 matches the phone number associated with the PayPal account for user william gauvin. The user of the william gauvin PayPal account sent money, as described above in paragraphs 14, 15, 18 and 19, to MV1 in exchange for the performance of sexual acts on camera.

27. The IP history provided by Google also reflects that, from October 27, 2016 until February 27, 2017, the IP address predominantly used to access the Gmail account [REDACTED]@gmail.com was 68.187.230.172.<sup>19</sup> After February 27, 2017, the next login date for the Gmail account [REDACTED]@gmail.com was March 6, 2017 and, on that date, the account was accessed by IP address 66.189.117.131. Between March 6, 2017 until April 9, 2017, the Gmail account was accessed either by IP address 66.189.117.131, or by IP addresses assigned to T-Mobile, a US Wireless Operator.<sup>20</sup> As described above, the IP addresses 68.187.230.172 and/or 66.189.117.131 were used to access the william gauvin PayPal account approximately 96 out of 113 times during the time period October 27, 2016 and March 22, 2017. In particular, IP address 68.187.230.172 was used on January 11, 2017 at 6:50 and 6:51 am UTC to send approximately \$300 and \$100 from william gauvin’s PayPal account to MV1’s PayPal account, and on February 24, 2017 at 5:10 am UTC, to send approximately \$500 from william gauvin’s PayPal account to MV1’s PayPal account as described in the text messages above.

---

<sup>19</sup> During that time frame, the Google records also show that, on several occasions, the Gmail account was accessed by IP address 207.30.52.199 which resolves back to a wireless provider. In my training and experience, this suggests that, on those occasions, the Gmail account was being accessed by a device that was not connected to a wireless network.

<sup>20</sup> In my training and experience, when the Gmail account was accessed by an IP address assigned to T-Mobile, it was being accessed by a device that was not connected to a wireless network.



28. Both IP addresses 68.187.230.172 and 66.189.117.131 are assigned to Charter Communications. In August 2017, HSI sent legal process to Charter Communications for subscriber information for IP address 68.187.230.172 on January 11, 2017 at 0551hrs (UTC), one of the dates and times when william gauvin's PayPal account sent money to MV1's PayPal account, as described in paragraphs 14 and 15 above.<sup>21</sup>

29. Charter Communications provided the following information regarding IP address 68.187.230.172 during the date/time requested:

IP address 68.187.230.172, 1/11/2017 5:51:00 AM, GMT, 0

Subscriber Name: MARC MERCADANTE  
Subscriber Address: [REDACTED], WORCESTER, MA 01602-1935  
Service Type - RR HSD Activate Date: 2/7/2008 Deactivate Date: Still Active  
User Name or Features: [REDACTED]@charter.net, [REDACTED]@charter.net  
Phone number: [REDACTED]-2261  
Advanced Subscriber Info  
Account Number: [REDACTED] 1517  
Equipment Details  
MAC: [REDACTED] a881  
Other Details  
Other Information:  
Lease Start Date: 10/21/2015, Lease End Date: 3/03/2017<sup>22</sup>

30. On Tuesday August 15, 2017 HSI Special Agent ("SA") Edward Bradstreet and

---

<sup>21</sup> The subpoena inadvertently sought records for January 11, 2017 at 5:51 UTC instead of 6:50 and 6:51 UTC. Regardless, as described herein, the results from Charter indicated that the IP address in question belonged to the same individual from 2015 through March 3, 2017.

<sup>22</sup> According to these records, this IP address was assigned to Mercadante, at the above address, during the entire lease period, including on January 10 and February 23 when william gauvin's PayPal account paid MV1 to engage in sexually explicit conduct using Skype, as described above. In addition to the records for the IP address ending in 172, HSI requested and Charter provided information regarding IP address 66.189.117.131 on March 6, 2017 at 0524 hrs (UTC) and April 9, 2017 at 0156 hrs (UTC). According to Charter records, as of March 3, 2017, IP address 66.189.117.131 was assigned to Mercadante, with the same information detailed above. The lease start date for this IP address was March 3, 2017 and the end date was September 5, 2017. Prior to March 3, 2017, this IP address belonged to a third party unrelated to this investigation.



Worcester Police Sgt. Brian Bisceglia conducted surveillance at [REDACTED], MA. A vehicle belonging to GAUVIN was not observed at that time. SA Bradstreet observed that the mailboxes to all the units of the 3-story building are located in an open common area accessible from [REDACTED] Street. The mailboxes for the Left units are located on the left side of the door while you walk in. The mailboxes for the R or right units are to the right of the door. The [REDACTED] mailbox was marked with a printed label taped on all four sides with:

[REDACTED]  
 Mercadante<sup>23</sup>  
 and  
 Gauvin

31. On Friday August 18, 2017, Worcester Police conducted surveillance at [REDACTED], Worcester, MA. In parking spot #3 agents observed a grey Toyota Corolla, Massachusetts license plate [REDACTED]. A query of the Massachusetts Registry of Motor Vehicles (RMV) database for this vehicle finds it is registered to the following person:

William GAUVIN  
 [REDACTED] Andover, MA 01810-1521<sup>24</sup>

32. On August 28, 2017 at approximately 0800hrs, Worcester Police conducted surveillance at [REDACTED], Worcester, MA. In parking spot #3 agents observed a grey Toyota Corolla, Massachusetts license plate [REDACTED].

33. Continuing on August 28, 2017 at approximately 2:25 pm, Worcester Police, HSI and FBI conducted surveillance at [REDACTED], Worcester, MA. Agents did not observe GAUVIN's car at that time. SA Bradstreet and Sgt. Bisceglia spoke with a resident of the

---

<sup>23</sup> Mercadante is an individual known to law enforcement to be living with GAUVIN.

<sup>24</sup> RMV Records indicate this address is a prior address for GAUVIN.

building, residing in unit [REDACTED], who confirmed that the letters “R” and “L” stood for “right” and “left” sides of the building (when viewed from the street or sidewalk). Thus, “2R/2L” indicated second floor, right or left and “3R/3L” indicated third floor right or left, with the stairway in between.

34. On August 29, 2017, SA Bradstreet reviewed Worcester Police Department Master Card Records for William GAUVIN. According to those records, on June 12, 2015, GAUVIN notified the Worcester Police that his motor vehicle, a Toyota Corolla, Massachusetts vehicle registration # [REDACTED], had been struck the night before at his residence [REDACTED] Worcester, MA 01602. His license information recorded in the report was MA # [REDACTED] 1594 and his date of birth was [REDACTED] 1975.

#### GAUVIN's History

35. On August 29, 2017, SA Bradstreet spoke with Lt. Gerald B. Roche, Jr. of the Billerica Police Department. SA Bradstreet also reviewed a report that Lt. Roche had submitted previously to the Worcester Police Department regarding William GAUVIN, date of birth [REDACTED] /1975, [REDACTED], Worcester, MA 01602-1935. According to that report, GAUVIN solicited a juvenile victim (“JV”) in the Town of Billerica in 2016. GAUVIN met JV on an online gay dating website called Grindr. The Grindr application allows users to create an account by users with or without using ones real name or real photo. Once the account is created, individuals can chat back and forth with the intent of possibly meeting in the future. In this instance, GAUVIN used a current photo of himself and went by the screen name “enjoy younger.” The JV also created an account using a current photo with the screen name “spoil younger” and he also identified himself as being 17 years of age. GAUVIN and the JV began their chat on August 14, 2016 via the Grindr application but eventually switched to “Skype” or

“Kik” to further communicate. Communication between JV and GAUVIN continued until August 26, 2016 when JV’s parents discovered messages on JV’s phone and took possession of the phone to stop the communication. JV’s father contacted the Billerica Police. Billerica Police interviewed JV with JV’s parents and took custody of the phone to review. JV admitted to sending photos of himself to GAUVIN for payment via a PayPal account that JV had set up. JV told Police he never sent nude pictures and that he always had shorts or underwear on. According to messages on JV’s phone between JV and a female friend, JV referred to GAUVIN as his “sugar daddy” and stated that this was “easy money.” JV further stated that he had opened up a second bank account for the purpose of depositing the funds from GAUVIN. JV’s phone also contained a photograph of JV holding a bank document with the words “sugar daddy account” written across it. Police added up the money that JV mentioned in the messages and it appears he was able to obtain approximately between \$1,500 and \$2,000 from GAUVIN.

**CHARACTERISTICS OF PERSONS WHO PRODUCE, RECEIVE AND POSSESS CHILD PORNOGRAPHY**

36. Based upon my training and experience, as well as from information provided to me by other law enforcement personnel involved in the investigation of cases involving the sexual exploitation of children, I believe the following traits and characteristics are generally found to exist and be true in cases involving individuals who produce, distribute, and/or collect child pornography:

- a. The majority of individuals who produce, distribute, receive and/or collect child pornography produce, distribute, and/or collect sexually explicit materials, which may consist of photographs, magazines, motion pictures, video tapes, books, slides, computer graphics or digital or other images for their own sexual gratification. The majority of these individuals also collect child erotica, which may consist of images or text that do not rise to the level of child pornography but which nonetheless fuel their deviant sexual fantasies involving children.



- b. The majority of individuals who produce, distribute, receive and/or collect child pornography often seek out like minded individuals, either in person or over the Internet, to share information and trade depictions of child pornography and child erotica as a means of gaining status, trust, acceptance and support. The different Internet based vehicles used by such individuals to communicate with each other include, but are not limited to: mobile applications, P2P, e-mail, e-mail groups, bulletin boards, Internet Relay Chat ("IRC"), newsgroups, instant messaging, and other similar vehicles.
- c. The majority of individuals who produce, distribute, receive and/or collect child pornography rarely, if ever, dispose of their sexually explicit materials and may go to great lengths to conceal and protect from discovery, theft, and damage their collections of illicit materials. They often maintain their collections in private and secure locations such as their homes or on electronic storage devices.
- d. Individuals who produce, distribute, receive and/or collect child pornography often use online resources to store child pornography, including online storage services offered by Apple, Microsoft, Inc., Yahoo! Inc., and Google, Inc., among others. The online storage services allow a user to set up an account with a remote computing service that provides electronic storage of computer files in a variety of formats. A user can set up an online storage account from any computer or cell phone with access to the Internet.

37. Based upon the facts described herein, there is probable cause to believe that GAUVIN produced, received and possessed child pornography in January and February 2017. Given the amount of money GAUVIN paid for the images, he clearly places great value on them and likely maintains them (including the corresponding text messages), as well as other images of child pornography, on his computer or other data storage device in his home to this day. Given the propensity of individuals who produce and receive child pornography to store such images within the privacy of their own homes, there is probable cause to believe that GAUVIN currently maintains the images he produced (including the associated text messages), and other images of

child pornography<sup>25</sup>, on a computer or other data storage device located within the SUBJECT PREMISES.

### **COMPUTER EVIDENCE**

38. Based upon my training and experience, I know that GAUVIN accessed Skype using some sort of electronic device – such as a computer, tablet, or smartphone – in order to entice MV1 to engage in sexually explicit conduct and to produce and receive images of child pornography.

39. Based upon the information provided by Charter, I know that some sort of electronic device was connected to the internet service provided by Charter at the SUBJECT PREMISES on January 11, 2017 at 6:50 and 6:51 am UTC and February 24, 2017 at 5:10 am UTC from IP address 68.187.230.172.

40. Computer hardware, other digital devices, software, and electronic files may be important to a criminal investigation in two distinct ways: (1) the objects themselves may be contraband, evidence, instrumentalities, or fruits of a crime; and / or (2) the objects may be used as storage devices that contain contraband, evidence, instrumentalities, or fruits of crime in the form of electronic data.

41. I know from training and experience that computers and magnetic and optical media are used to store information. In addition to the above mentioned image files, that information often includes data files of other persons engaged in similar activities with minors, and lists of other exploited juveniles, as well as records of correspondence and conversations (printed or electronic) with such persons.

---

<sup>25</sup> It is particularly likely that GAUVIN's home will contain other images of child pornography in light of GAUVIN's prior use of a computer to produce and receive, at the very least, images of child erotica as described in paragraph 35 with respect to JV.



42. In this case, the search warrant application requests permission to search and seize digital media files which constitute evidence of the TARGET OFFENSES as further described in Attachment B, including those items that may be stored on a computer, digital device or on electronic media. The images involving sexual conduct of minors constitute both evidence of crime and contraband.

43. I know from training and experience that computer systems commonly consist of computer processing units ("CPUs"), hard disks, hard disk drives, floppy disk drives, tape drives, display screens, keyboards, printers, modems (used to communicate with other computers), electronic cables, cassette tapes, floppy disks, and other forms of magnetic and optical media contain computer information. In addition, the specific transmission of computerized imagery indicates the possible use of CD-ROM / DVD drives, compact laser disks, image scanning devices, still cameras, lighting equipment, video cameras or camcorders, VCRs, digital-analogue translation devices, and the software (computer programming) necessary to operate them.

44. Based on my training, experience, and information provided by other law enforcement officers, I know that many smartphones (which are included in Attachment B's definition of "computer hardware") can now function essentially as small computers. Smartphones have capabilities that include serving as a wireless telephone, digital camera, portable media player, GPS navigation device, sending and receiving text messages and e-mails, and storing a vast range and amount of electronic data. Examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

45. Based on my knowledge, training, experience, and information provided to me by other agents, I know that computer files or remnants of such files can be recovered months or years after



they have been written, downloaded, saved, deleted, or viewed locally or over the Internet. This is true because:

- a. Electronic files that have been downloaded to a storage medium can be stored for years at little or no cost. Furthermore, when users replace their computers, they can easily transfer the data from their old computer to their new computer.
- b. Even after files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person “deletes” a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data, which might not occur for long periods of time. In addition, a computer's operating system may also keep a record of deleted data in a “swap” or “recovery” file.
- c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how the computer has been used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. It is technically possible to delete this information, but computer users typically do not erase or delete this evidence because special software is typically required for that task.
- d. Similarly, files that have been viewed over the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.” The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are overwritten only as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

**Need for Computer Equipment to be Seized and Searched Off-Site**

46. This affidavit also requests permission to seize the computer hardware and storage media that may contain the evidence described in Attachment B if it becomes necessary for reasons of practicality to remove the hardware and conduct a search off-site. I believe that, in this case, the computer and digital hardware is a container for evidence, a container for contraband and also itself an instrumentality of the crime under investigation.

47. Based on my knowledge and training and the experience of other agents with whom I have spoken, I am aware that in order to completely and accurately retrieve data maintained in computer hardware, computer software or storage media, to ensure the accuracy and completeness of such data, and to prevent the loss of the data either from accidental or programmed destruction, it is often necessary that computer hardware, computer software, and storage media (“computer equipment”) be seized and subsequently processed by a computer specialist in a laboratory setting rather than in the location where it is seized. This is true because of:

- a. The volume of evidence — storage media such as hard disks, flash drives, CDs, and DVDs can store the equivalent of thousands or, in some instances, millions of pages of information. Additionally, a user may seek to conceal evidence by storing it in random order or with deceptive file names. Searching authorities may need to examine all the stored data to determine which particular files are evidence, fruits, or instrumentalities of criminal activity. This process can take weeks or months, depending on the volume of data stored, and it would be impractical to attempt this analysis on-site.
- b. Technical requirements — analyzing computer hardware, computer software or storage media for criminal evidence is a highly technical process requiring expertise and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications. Thus, it is difficult to know, before the search, which expert possesses sufficient specialized skill to best analyze the system and its data. Furthermore, data analysis protocols are exacting procedures, designed to protect the integrity of the evidence and to recover even “hidden,” deleted, compressed, or encrypted files. Many commercial computer software programs also save data in unique formats that are not conducive to standard data searches. Additionally, computer evidence is extremely vulnerable to tampering or destruction, both from external sources and destructive code imbedded in the system as a “booby trap.”

Consequently, law enforcement agents may either copy the data at the premises to be searched or seize the computer equipment for subsequent processing elsewhere.

48. The premises may contain computer equipment whose use in the crime(s) or storage of the things described in this warrant is impractical to determine at the scene. Computer equipment and data can be disguised, mislabeled, or used without the owner’s knowledge. In



addition, technical, time, safety, or other constraints can prevent definitive determination of their ownership at the premises during the execution of this warrant. If the things described in Attachment B are of the type that might be found on any of the computer equipment, this application seeks permission to search and seize it onsite or off-site in order to determine their true use or contents, regardless of how the contents or ownership appear or are described by people at the scene of the search.

49. Based on my training and experience, and discussions with members of the HSI cyber crimes unit, I know that a qualified computer specialist is required to properly retrieve, analyze, document and authenticate electronically stored data, and to prevent the loss of data either from accidental or deliberate programmed destruction. To do this work accurately and completely requires the seizure of (1) all computer equipment and peripherals, which may be interdependent; (2) the software to operate the computer system(s); (3) the instruction manuals, which contain directions concerning the operation of the computer system(s) and software programs; and, (4) all internal and external data storage devices. Each of the seized items should be searched in a laboratory or controlled environment.

50. Searching computer systems for criminal evidence is a highly technical process requiring expert skill and a significant amount of time. Indeed, computer specialists, using exacting data search protocols, must often recover hidden, erased, compressed, password-protected, or encrypted files in order to find evidence of criminal activity. Moreover, many commercial computer software programs save data in unique formats that are not conducive to standard data searches. This requires additional effort by specialists to review such data for evidence of a crime. Finally, many users try to conceal criminal evidence by storing files in random order with deceptive file names. This requires specialists to examine all of a user's stored data to determine



which particular files are relevant and within the scope of the search warrant. This process can take a substantial amount of time depending on the volume of data stored.

51. Because computer evidence is extremely vulnerable to tampering or destruction, both from external sources or from destructive codes imbedded in the system as “booby traps,” a controlled environment is essential to a complete and accurate analysis.

52. For the reasons described in the Computer Evidence section of this affidavit, it is necessary to seize all computers, data storage devices and related equipment, as described in Attachment B. It is further necessary to search such equipment in a controlled environment, off-site. Given the potential for large quantities of data, a complete forensic examination of the seized items will take longer than fourteen days.

#### **Return of Seized Computer Equipment**

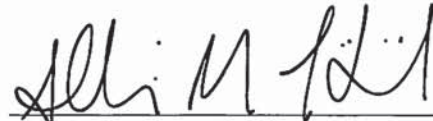
53. To the extent practical, if persons claiming an interest in the seized computers so request, I will make available to those individuals copies of requested files (so long as those files are not considered contraband) within a reasonable time after the execution of the search warrant. In addition, as soon as practical, those items of hardware and software no longer required for the purpose of analysis or copying of items authorized to be seized, or for the preservation of the data and/or magnetic evidence, will be returned to the party from which they were seized, so long as such items do not constitute contraband.

54. In the instant case, I submit that there is probable cause to believe that GAUVIN committed the TARGET OFFENSES using a computer or smartphone in, at least, January and February 2017. Based on my training and experience, I submit that there is probable cause to believe that evidence of the TARGET OFFENSES is currently present on his computer or other data storage devices within his home even if GAUVIN deleted the files.

**CONCLUSION**


55. Based on the foregoing, I respectfully submit that there is probable cause to believe that evidence, fruits and instrumentalities of the TARGET OFFENSES will be found at the SUBJECT PREMISES. Such evidence, fruits and instrumentalities are more fully described in Attachment B attached hereto.

56. WHEREFORE, your affiant requests that warrants issue to search the SUBJECT PREMISES for the items described in Attachment B and attached hereto.




Special Agent Allison M. Haimila  
Department of Homeland Security  
Homeland Security Investigations

Subscribed and sworn to before me this 31st day of October, 2017



HONORABLE DAVID H. HENKEN  
CHIEF, UNITED STATES MAGISTRATE JUDGE



IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF MASSACHUSETTS

In The Matter of the Search of

  
Worcester, Massachusetts

M.J. No. 17-mj-4285-DHH

MOTION TO UNSEAL IN REDACTED FORM

The United States of America respectfully moves this Court to unseal the search warrant application, supporting affidavit, search warrant, this motion, any ruling on this motion, and all related paperwork until further order of this Court, in redacted form. In support of this motion, the government states that the defendant has been arrested and there is no longer a need to keep these materials sealed. The materials, however, contain personal identifying information of the defendant (*e.g.*, the defendant's street address, date of birth and social security number) which should not be made public and, therefore, have been redacted to protect such information from disclosure. Redacted copies of the materials, to be filed, are attached hereto as Exhibit 1.

The United States further moves, pursuant to General Order 06-05, that the United States Attorney, through undersigned counsel, be provided copies of all sealed documents which the United States has filed in this matter.

Respectfully submitted,

WILLIAM D. WEINREB  
Acting United States Attorney

By: /s/ Karin M. Bell  
KARIN M. BELL  
Assistant U.S. Attorney

Date: November 1, 2017